CS 198 Codebreaking at Cal
Spring 2023 Homework

HW 1

Question 1

Explain why an attacker familiar with the steganography scheme being used has full ability to read and tamper with messages.

Question 2

Recall that a *simple substitution cipher* is any function $F : A \to A$ that maps elements of A to A (as a bijection). This does not have to be a consistent "shift" like a Caesar cipher, only some function that takes in a letter and spits out another letter (uniquely). For our purposes, we only want to consider English lowercase alphabets, so 26 possible elements of A.

An example simple substitution cipher [1]:

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**

A would map to D, and so forth.

How many different simple substitution ciphers are there?

Question 3

Research and learn about a new hand cipher (an encryption scheme usable by a human without a computer), encrypt a short (< 20 character message) with a key of your choosing by hand, and leave the message below!

Mention briefly which cipher you used and why you found it interesting, and explain how encryption/decryption works in said cipher.

Contributors:

- Ryan Cottone

[1] Credit https://www.cimt.org.uk/resources/codes/codes_u1_text.pdf